IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPEAL FROM THE EXAMINER
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants:	Neal A. KRAWETZ	Confirmation No.: 9182
Application Serial No.:	09/975,815	
Filed:	October 11, 2001	
Title:	SYSTEM AND METHOD FOR SECURE DATA TRANSMISSION	
Group Art Unit:	2136	
Examiner:	Colin, Carl	
Docket No.:	10019968-1	

MAIL STOP: APPEAL BRIEF PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

APPEAL BRIEF

Appellant has appealed to the Board of Patent Appeals and Interferences from the decision of the Examiner mailed June 12, 2008, finally rejecting Claims 1-34. Appellant filed a Notice of Appeal on August 11, 2008. Appellant respectfully submits this Appeal Brief with authorization to charge the statutory fee of $540.00.

REAL PARTY IN INTEREST

The present application was assigned to Hewlett-Packard Company recorded on March 14, 2002 in the Assignment Records of the United States Patent and Trademark Office at Reel 012730, Frame 0935. The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

STATUS OF CLAIMS

Claims 1-34 stand rejected pursuant to a final Office Action mailed June 12, 2008 ("Office Action"). Claims 1-34 are presented for appeal.

STATUS OF AMENDMENTS

No amendment has been filed subsequent to the mailing of the Final Office Action.

SUMMARY OF CLAIMED SUBJECT MATTER

Appellant advises the Board that the line number references noted below have been determined by counting only the lines of text on the pages of the originally filed application.

Embodiments of the present invention as defined by independent Claim 1 are directed toward a method for secure data transmission (Pg. 7, lines 13-14; Fig. 2) comprising generating a character string (Pg. 4, lines 19-20; pg. 7, lines 18-19; Fig. 2, Ref. 208) at a sender (Pg. 3, lines 22-24; Fig. 1, Ref. 18) for each data packet associated with the secure data transmission (Pg. 8, lines 25-27; Fig. 2), generating a hash key using the character string and a private key (Pg. 4, lines 20-21; pg. 7, lines 19-20; Fig. 2, Ref. 210), wherein the hash key is different for each data packet associated with the secure data transmission (Pg. 8, lines 25-27; Fig. 2), encrypting a data packet associated with the secure data transmission using the hash key (Pg. 4, lines 22-23; pg. 7, lines 21-22; Fig. 2, Ref. 212), and transmitting an identification key

associated with the sender, the character string, and the encrypted data packet from the sender to a recipient (Pg. 4, lines 24-26; pg. 7, lines 24-26; Fig. 2, Ref. 216).

Embodiments of the present invention as defined by independent Claim 11 are directed toward a method for secure data transmission (Pg. 7, lines 27-28; Fig. 3) comprising receiving a plurality of character strings from a sender (Pg. 7, line 31; Pg. 8, lines 1-2, 25-27; Fig. 3. Ref. 304), receiving an identification key from the sender (Pg. 7, line 31; Pg. 8, lines 1-2; Fig. 3. Ref. 304), receiving a plurality of encrypted data packets from the sender (Pg. 7, line 31; Pg. 8, lines 1-2; Fig. 3. Ref. 304), each of the plurality of character strings correspond to one of the plurality of encrypted data packets (Pg. 8, lines 25-27; Fig. 3), determining a private key associated with the sender using the identification key (Pg. 8, lines 4-5; Fig. 3, Ref. 308), and decrypting the plurality of encrypted data packets using the private key and the respective character strings (Pg. 8, lines 7-9; Fig. 3, Ref. 312).

Embodiments of the present invention as defined by independent Claim 19 are directed toward a system for secure data transmission (Pg. 3, lines 9-10; Fig. 1, Ref. 10) comprising a processor (Pg. 3, lines 20-21; Fig. 1, Ref. 30), a memory coupled to the processor (Pg. 3, lines 20-21; Fig. 1, Ref. 32), a string generator stored in the memory and executable by the processor (Pg. 3, lines 22-27; Fig. 1, Ref. 40), the string generator adapted to generate a character string (Pg. 4, lines 19-20), a hashing engine stored in the memory and executable by the processor (Pg. 3, lines 22-27; Fig. 1, Ref. 42), the hashing engine adapted to generate a hash key using the character string and a private key (Pg. 4, lines 20-22), wherein the hash key is different for each data packet associated with the secure data transmission (Pg. 8, lines 25-27), and an encryption engine stored in the memory and executable by the processor (Pg. 3, lines 22-27; Fig. 1, Ref. 44), the encryption engine adapted to encrypt the data using the hash key (Pg. 4, lines 22-23), and wherein the processor is adapted to transmit the encrypted data, an identification key related to the private key, and the character string to a recipient.

Embodiments of the present invention as defined by independent Claim 27 are directed toward a system for secure data transmission (Pg. 3, lines 9-10; Fig. 1, Ref. 10) comprising a processor (Pg. 5, lines 4-5; Fig. 1, Ref. 80) adapted to receive a plurality of encrypted data packets, an identification key, and a plurality of character strings (Pg. 7, line 31; Pg. 8, lines 1-2, 25-27; Fig. 1, Refs. 72, 60, 54) from a sender (Pg. 3, lines 22-24; Fig. 1, Ref. 18), each of the plurality of character strings correspond to one of the plurality of encrypted data packets (Pg. 4, lines 19-26; pg. 8, lines 25-27), a memory coupled to the processor (Pg. 5, lines 4-5; Fig. 1,

Ref. 82), a relational database stored in the memory and accessible by the processor (Pg. 5, lines 18-20; Fig. 1, Ref. 102), the relational database relating the identification key to a private key (Pg. 5, lines 20-27) and a decryption engine stored in the memory and executable by the processor (Pg. 5, lines 9-11; Fig. 1, Ref. 88), the decryption engine adapted to decrypt the encrypted data packets using the respective character strings and the private key (Pg. 8, lines 5-9).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-34 are rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement.

2. Claims 1-2, 4-5, 7-8, 11-12, 14-15, 19 and 22-25 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,931,128 to Roberts (hereinafter "*Roberts*").

3. Claims 3, 6, 9-10, 13, 16-18, 20-21 and 26-34 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Roberts* in view of U.S. Patent No. 6,751,736 to Bowman, et al. (hereinafter "*Bowman*").

ARGUMENT

A. Standard

1. 35 U.S.C. § 112, first paragraph

The "specification shall contain a written description of the invention." MPEP §2163. To satisfy the written description requirement, a patent specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. *See*, e.g., *Moba, B.V. v. Diamond Automation, Inc.*, 325 F.3d 1306, 1319, 66 USPQ2d 1429, 1438 (Fed. Cir. 2003). An Appellant shows possession of the claimed invention by describing the claimed invention with all of its limitations using such descriptive means as words, structures, figures, diagrams, and formulas that fully set forth the claimed invention. *Lockwood v. American Airlines, Inc.*, 107 F.3d 1565, 1572, 41 USPQ2d 1961, 1966 (Fed. Cir. 1997). It is not necessary that the claimed subject matter be described identically but that the originally filed disclosure convey to those skilled in the art that appellant had invented the subject matter now claimed. *In re Wertheim*, 541 F.2d 257, 191 USPQ 90 (C.C.P.A. 1976). "Satisfaction of the 'written description' requirement does not require *in haec verba* antecedence in the originally filed application." *Staehelin V. Secher*, 24 USPQ2d

1513 (Bd. Pat. App. & Inter. 1992). The exact words in question in a claim need not appear in the specification. *In re Wright*, 866 F.2d 422, 425, 9 USPQ2d 1649, 1651 (Fed. Cir. 1989) ("The fact, therefore, that the exact words here in question, 'not permanently fixed', are not in the specification is not important."). There is a strong presumption that an adequate written description of the claimed invention is present when the application is filed. *In re Wertheim*, 541 F.2d 257, 263, 191 USPQ 90, 97 (CCPA 1976) (emphasis added).

Moreover, a description as filed is presumed to be adequate, unless or until sufficient evidence or reasoning to the contrary has been presented by the Examiner to rebut the presumption. *See, e.g., In re Marzocchi*, 439 F.2d 220, 224, 169 USPQ 367, 370 (C.C.P.A. 1971). The Examiner, therefore, must have a reasonable basis to challenge the adequacy of the written description, and the Examiner has the initial burden of presenting by a preponderance of evidence why a person skilled in the art would not recognize in Appellant's disclosure a description of the invention defined by the claims. *In re Wertheim*, 541 F.2d 257, 263, 191 USPQ 90, 97 (C.C.P.A. 1971); MPEP §2163.04. In rejecting a claim, the Examiner must set forth express findings of fact which support the lack of written description conclusion and should: (A) identify the claim limitation at issue; and (B) establish a *prima facie* case by providing reasons why a person skilled in the art at the time the application was filed would not have recognized that the inventor was in possession of the invention as claimed in view of the disclosure of the application as filed. See MPEP §2163.04(I).

2. 35 U.S.C. §102

Under 35 U.S.C. § 102, a claim is anticipated only if each and every element as set forth in the claim is found in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987); M.P.E.P. § 2131. In addition, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claims" and "[t]he elements must be arranged as required by the claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. § 2131.

3. 35 U.S.C. §103

The Examiner bears the burden of establishing a prima facie case of obviousness based on the prior art when rejecting claims under 35 U.S.C. §103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Additionally, all limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d

1031, 1034 (Fed. Cir. 1994). Therefore, no *prima facie* obviousness rejection can be established if the proposed combination does not teach all of the features of the claimed invention. Additionally, rejections based on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *Teleflex Inc. v. KSR Int'l Co.*, 550 U.S. __, __, 82 U.S.P.Q.2d 1385, 1396 (2007).

B. Argument

1. Rejection under 35 U.S.C. § 112

a. Claims 1-34

Claims 1-34 are rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. On page 3 of the Office Action, Appellee appears to assert that subject matter added to Claims 1, 11, 19 and 27 by Appellant in the Response filed February 15, 2008 ("Response") was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor, at the time the application was filed, had possession of the claimed invention.

Appellant amended Claim 1 in the Response to add the following underlined limitations: "generating a character string at a sender for each data packet associated with the secure data transmission," "generating a hash key using the character string and a private key, wherein the hash key is different for each data packet associated with the secure data transmission," and "encrypting a data packet associated with the secure data transmission using the hash key." Appellant expressly indicated on page 8 of the Response that support for the amendments was found in the originally-filed specification on at least page 8, lines 25-27. Regardless, Appellee asserts on page 3 of the Office Action that the originally-filed specification fails to provide support for the above-noted claim limitations. Specifically, Appellee states that "there is no description in the disclosure for specifying which part of the encryption key changes for each data packet and there is no disclosure of data packet associated with the secure transmission." Appellant respectfully disagrees.

On page 8, in lines 25-27, of the originally-filed disclosure, Appellant states that "unlike secure shell or other tunneling protocols, the encryption key changes with each transmitted data packet" (emphasis added). As disclosed on page 4, lines 20-22, and illustrated in block 210 of Fig. 2, the encryption key (a.k.a., the hash key 64) is generated using the

character string 54 and the private key 62. Appellant submits that one skilled in the art would recognize that the variable used to generate the hash key 64, namely the character string 54, is changed to generate a hash key 64 that "changes with each transmitted data packet" as expressly disclosed on page 8, in lines 25-27, of the originally-filed disclosure. For example, at least on page 4 of the originally-filed disclosure, it is stated that "the string generator randomly generates and stores the character string," and that the character string is hashed with the private key to generate the hash key (page 4, lines 19-33). Moreover, one skilled in the art would recognize that the encrypted data packets are associated with the secure transmission.

Based on the foregoing, Appellant submits that Appellee's rejection of Claim 1 does not appear to be well founded. Therefore, Appellant respectfully requests that the Board reverse Appellee's § 112, 1st paragraph, rejection of Claim 1.

On page 3 of the Office Action, Appellee appears to reject independent Claims 11, 19 and 27 for the same or similar reasons as Claim 1 was rejected. At least for the reasons discussed above in connection with independent Claim 1, Appellant respectfully submits that the amendments to Claims 11, 19 and 27 in the Response are also supported by the originally-filed specification. As such, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 11, 19 and 27.

Each of Claims 2-10, 12-18, 20-26 and 28-34, either directly or through intervening claims, depends from and includes all the base limitations of independent Claims 1, 11, 19 and 27, respectively. As such, each of Claims 2-10, 12-18, 20-26 and 28-34 is believed to comply with the written description requirement of § 112, 1st paragraph, for at least the reasons noted above for Claims 1, 11, 19 and 27. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 2-10, 12-18, 20-26 and 28-34.

2. Rejection under 35 U.S.C. §102(e) over *Roberts*

Claims 1-2, 4-5, 7-8, 11-12, 14-15, 19 and 22-25 are rejected under 35 U.S.C. §102(e) as being anticipated by *Roberts*.

a. Claims 1-2, 4 and 8

Of the rejected claims, Claim 1 is independent. For the reasons set forth below, Appellant respectfully submits that Claim 1 is patentable at least because *Roberts* does not appear to disclose or suggest each and every element as set forth in independent Claim 1.

Claim 1 recites, *inter alia*, "transmitting an identification key associated with the sender, the character string, and the encrypted data packet from the sender to a recipient" (emphasis added). On pages 4-5 of the Office Action, Appellee appears to assert that *Roberts* discloses this limitation by "transmitting an identification key (SPI)." However, in Col. 9, line 65 through Col. 10, line 7, *Roberts* states:

> A Secure Parameter Index (SPI) is a 96 bit (12 byte) bit sequence that is unique to the second computer system. The SPI may be included to ensure compatibility with the Encapsulation Security Payload (ESP) protocol of the Internet Protocol Security (IPSec) protocol ... The data packet 204 is then transmitted to the second computer system (act 409) for decryption by the decryption device 202.

(emphasis added).

Therefore, the Secure Parameter Index (SPI) of *Roberts* appears to be associated with the second computer, i.e., the receiving computer, and does not appear to be "associated with the sender" as recited in Claim 1. For at least this reason, *Roberts* does not appear to anticipate Claim 1. As such, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 1.

Each of Claims 2, 4 and 8, either directly or through intervening claims, depends from and includes all the base limitations of independent Claim 1. As such, each of Claims 2, 4 and 8 is believed to be patentable for at least the reasons noted above for Claim 1. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 2, 4 and 8.

b. Claims 5 and 7

Appellant respectfully submits that Claims 5 and 7 are patentable at least because *Roberts* does not appear to disclose or suggest each and every element as set forth in Claims 5 and 7.

Each of Claims 5 and 7 recites, *inter alia*, "determining the private key at the recipient using the identification key." On page 5 of the Office Action, Appellee appears to equate the "identification key" as recited in Claims 5 and 7 to the Secure Parameter Index (SPI) of *Roberts* and asserts that *Roberts* discloses the above-quoted limitation of Claim 5 in Col. 6, lines 45-54, and Col. 9, lines 58-67. Appellant respectfully disagrees. In Col. 6, lines 45-54, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be negotiated in the same

session as when the first and second computer securely negotiate a master secret. In addition, in Col. 9, lines 58-67, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be included in the data packet to ensure compatibility with the Encapsulation Security Payload (ESP) protocol of the Internet Protocol Security (IPSec) protocol. Therefore, Appellee has not pointed out, and Appellant is unable to locate, any teaching or suggestion in *Roberts* that the Secure Parameter Index (SPI) is used in "determining the private key at the recipient using the identification key" as recited in Claims 5 and 7. Therefore, *Roberts* does not appear to anticipate Claims 5 and 7. As such, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 5 and 7.

Also, each of Claims 5 and 7, either directly or through intervening claims, depends from and includes all the base limitations of independent Claim 1. As such, each of Claims 5 and 7 is believed to be patentable for at least the reasons noted above for Claim 1. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 5 and 7.

c. Claims 11, 12 and 14-15

Of the rejected claims, Claim 11 is independent. For the reasons set forth below, Appellant respectfully submits that Claim 11 is patentable at least because *Roberts* does not appear to disclose or suggest each and every element as set forth in independent Claim 11.

Claim 11 recites, *inter alia*, "receiving an identification key from the sender" and "determining a private key associated with the sender using the identification key" (emphasis added). On pages 6-7 of the Office Action, Appellee appears to equate the "identification key" as recited in Claim 11 to the Secure Parameter Index (SPI) of *Roberts*. As noted above, in Col. 9, line 65 through Col. 10, line 7, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be included in the data packet to ensure compatibility with the Encapsulation Security Payload (ESP) protocol of the Internet Protocol Security (IPSec) protocol. In addition, in Col. 6, lines 45-54, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be negotiated in the same session as when the first and second computer securely negotiate a master secret. However, Appellee has not pointed out, and Appellant is unable to locate, any teaching or suggestion in *Roberts* that the Secure Parameter Index (SPI) is used in "determining a private key associated with the sender" as recited in Claim 11. For at least this reason, *Roberts* does not appear to anticipate Claim 11. As such, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 11.

Each of Claims 12 and 14-15, either directly or through intervening claims, depends from and includes all the base limitations of independent Claim 11. As such, each of Claims 12 and 14-15 is believed to be patentable for at least the reasons noted above for Claim 11. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 12 and 14-15.

d. Claims 19 and 22-24

Of the rejected claims, Claim 19 is independent. For the reasons set forth below, Appellant respectfully submits that Claim 19 is patentable at least because *Roberts* does not appear to disclose or suggest each and every element as set forth in independent Claim 19.

Independent Claim 19 recites "wherein the processor is adapted to transmit the encrypted data, an identification key related to the private key, and the character string to a recipient" (emphasis added). On pages 6-7 of the Office Action, Appellee appears to equate the "identification key" as recited in Claim 11 to the Secure Parameter Index (SPI) of *Roberts*. As noted above, in Col. 9, line 65 through Col. 10, line 7, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be included in the data packet to ensure compatibility with the Encapsulation Security Payload (ESP) protocol of the Internet Protocol Security (IPSec) protocol. In addition, in Col. 6, lines 45-54, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be negotiated in the same session as when the first and second computer securely negotiate a master secret. However, Appellee has not pointed out, and Appellant is unable to locate, any teaching or suggestion in *Roberts* that the Secure Parameter Index (SPI) is "related to the private key" as recited in Claim 19. For at least this reason, *Roberts* does not appear to anticipate Claim 19. As such, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 19.

Each of Claims 22-24, either directly or through intervening claims, depends from and includes all the base limitations of independent Claim 19. As such, each of Claims 22-24 is believed to be patentable for at least the reasons noted above for Claim 19. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 22-24.

e. Claim 25

Appellant respectfully submits that Claim 25 is patentable at least because *Roberts* does not appear to disclose or suggest each and every element as set forth in Claim 25.

Claim 25 recites, *inter alia*, "the recipient is adapted to determine the hash key using the identification key and the character string." On page 8 of the Office Action, Appellee appears to equate the "identification key" as recited in Claim 25 to the Secure Parameter Index (SPI) of *Roberts* and asserts that *Roberts* discloses the above-quoted limitation of Claim 25 in Col. 6, lines 45-54, and Col. 9, lines 62-67. Appellant respectfully disagrees. In Col. 6, lines 45-54, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be negotiated in the same session as when the first and second computer securely negotiate a master secret. In addition, in Col. 9, lines 58-67, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be included in the data packet to ensure compatibility with the Encapsulation Security Payload (ESP) protocol of the Internet Protocol Security (IPSec) protocol. Therefore, Appellee has not pointed out, and Appellant is unable to locate, any teaching or suggestion in *Roberts* that the Secure Parameter Index (SPI) is useable by the recipient "to determine the hash key" as recited in Claim 25. Therefore, *Roberts* does not appear to anticipate Claim 25. As such, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 25.

Also, Claim 25 depends from and includes all the base limitations of independent Claim 19. As such, Claim 25 is believed to be patentable for at least the reasons noted above for Claim 25. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 25.

3. Rejection under 35 U.S.C. §103(a) over *Roberts* in view of *Bowman*

Claims 3, 6, 9, 10, 13, 16-18, 20-21 and 26-34 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Roberts* in view of *Bowman*.

a. Claims 27 and 28-34

Of the rejected claims, Claim 27 is independent. For the reasons set forth below, Appellant respectfully submits that Claim 27 is patentable over *Roberts* in view of *Bowman* because neither *Roberts* nor *Bowman*, alone or in combination, appears to disclose or suggest each and every element as set forth in independent Claim 27.

Claim 27 recites, *inter alia*, "a processor adapted to receive ... an identification key ... from a sender." (emphasis added). On page 4, lines 9-11, of the originally-filed specification, Appellant indicates that the "identification key 60 may comprise a serial number or other type of identifier indicating the particular client 18 transmitting the data" (emphasis added). On page 16 of the Office Action, Appellee appears to equate the "identification key" as recited in Claim 27 to

the Secure Parameter Index (SPI) of *Roberts*. However, in Col. 6, lines 45-54, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be negotiated in the same session as when the first and second computer securely negotiate a master secret. In addition, in Col. 9, lines 58-67, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be included in the data packet to ensure compatibility with the Encapsulation Security Payload (ESP) protocol of the Internet Protocol Security (IPSec) protocol. Appellee has not pointed out, and Appellant is unable to locate, any teaching or suggestion in *Roberts* that the Secure Parameter Index (SPI) is employed as "an identification key" as recited in Claim 27, much less an identification key identifying a particular client as defined by the originally-filed specification. In addition, *Roberts* indicates in Col. 9, lines 65-67, that the "Secure Parameter Index (SPI) is a 96 bit (12 byte) bit sequence that is unique to the second computer system" (emphasis added). Appellants submit that, if the Secure Parameter Index (SPI) is unique to the second computer system as indicated, then there is no reason to send the SPI to identify the sender or to "receive ... an identification key ... from a sender" as recited in Claim 27.

Based on the foregoing, Appellant asserts that *Roberts* fails to disclose or even suggest each and every limitation recited in Claim 27. Moreover, *Bowman* does not appear to overcome this deficiency of *Roberts*. Therefore, Claim 27 is believed to be patentable over the combination of *Roberts* and *Bowman*. As such, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 27.

In addition, Appellant respectfully submits that one skilled in the art would not combine *Roberts* with *Bowman*. Indeed, in Col. 6, lines 46-49, *Roberts* states:

> As illustrated by FIG. 4, before secure communications begin, the first and second computer system securely negotiate a master secret (act 401) that is to be known by only the first and second computer systems.

(emphasis added).

Therefore, *Roberts* appears to disclose that the master secret is negotiated between the first and second computers prior to the commencement of any secure communications. Appellant submits that the exchange of the master secret of *Roberts* outside of secure communications avoids the possibility that the master secret, which is used to decrypt the encrypted information, could be intercepted at the same time as the encrypted information during transmission.

In contrast, in Col. 9, lines 18-20, *Bowman* states:

> Referring to FIG. 7 an algorithm for decoding, decrypting, and authenticating the VBC produced by the algorithm of FIG. 6 is represented. In block 711 VBC is received after being parsed from a received HTTP message, which may include selected option name value pairs. In block 714, the received VBC is decoded (e.g., base 64 decoded) to produce a binary string from received character string, and in block 717 the binary string is parsed to separate the encrypted string, 721, the random sting, 724, and the secret ID 727. The secret ID is used as an index into a database in block 730 to access the corresponding secret string, 733.

(emphasis added).

Based on the above, *Bowman* appears to disclose that secret ID 727 is transmitted along with and as a part of the encrypted virtual bar code (VBC), which includes the sensitive name/value pair information sought to be protected. Appellant submits that because the secret ID 727, which is used to decrypt the VBC, is transmitted along with the encrypted bar code (VBC), one skilled in the art would not look to combine *Roberts* with *Bowman* as suggested by Appellee. Indeed, because the master secret of *Roberts* was negotiated outside of a secure transmission containing the sensitive information, there is no rationale to support adding the relational database of *Bowman* to discourage loss of sensitive information due to simultaneous interception of the sensitive information and the key that unlocks the same.

Claims 28-34, either directly or through intervening claims, depends from and includes all the base limitations of independent Claim 27. As such, each of Claims 28-34 is believed to be patentable for at least the reasons noted above for Claim 27. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 28-34.

b. Claims 3, 10 and 20

Claims 3 and 10 recite, *inter alia*, "generating a signature using the hash key and the data." In addition, Claim 20 recites, *inter alia*, "the signature engine adapted to generate a signature using the hash key and the data." On pages 9, 11-12 and 15 of the Office Action, Appellee appears to acknowledge that *Roberts* does not teach or even suggest this limitation. Appellant agrees. However, Appellee asserts that *Bowman* overcomes this deficiency. Appellant respectfully disagrees.

On pages 9, 11-12 and 15 of the Office Action, Appellee indicates that the above-quoted limitation of Claims 3, 10 and 20 is disclosed in Col. 7, lines 59-67, of *Bowman*, which states:

> The secret ID, random string, and encrypted VBC string are then concatenated in block 437. In block 438 the concatenated string is character encoded, e.g., by Base 64 encoding, to form the virtual bar code. Base64 encoding has the advantage that the resulting character string is made up of character common to ASCII, EBCDIC and other character sets used by computers around the world through which HTTP messages may be routed.

However, Appellee has not specifically pointed out, and Appellant is unable to determine, where a "signature" as recited in Claims 3, 10 and 20 is included in the quoted portion of *Bowman*. Moreover, Appellee has not specifically pointed out, and Appellant is unable to determine, where "data" as recited in Claims 3, 10 and 20 is included in the quoted portion of *Bowman*. According to 37 C.F.R. §1.104(c)(2):

> The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified.

In fact, the goal of examination is to clearly articulate any rejection early in the prosecution process so that Appellant has the opportunity to provide evidence of patentability and otherwise reply completely at the earliest opportunity. See MPEP §706. Because the quoted portion of *Bowman* does not appear to teach or even suggest the limitations of Claims 3, 10 and 20, which also do not appear to have been properly rejected, the Board should overturn Appellee's rejection of Claims 3, 10 and 20.

In addition to the above, on pages 9, 11-12 and 15 of the Office Action, Appellee appears to acknowledge that neither *Roberts* nor *Bowman*, either alone in combination, discloses "generating a signature using the hash key and the data." Indeed, Appellee states that the "difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key" (emphasis in original). However, on pages 9, 11-12 and 15 of the Office Action Appellee indicated that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for better security." Appellants respectfully disagree. Indeed, if one skilled in the art would have used the hash key instead of the private key to generate better security as suggested by Appellee, then Appellant submits that *Bowman* would have used the hash key instead of the

private key to generate the signature. Because *Bowman* did not use the hash key in favor of the private key, as acknowledged by Appellee, Appellant submits that Appellee's reasoning and rationale for modifying *Roberts* is not well founded. As such, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 3, 10 and 20.

Claims 3, 10 and 20, either directly or through intervening claims, depends from and includes all the base limitations of independent Claims 1 and 19, respectively. As such, each of Claims 3, 10 and 20 is believed to be patentable for at least the reasons noted above for Claims 1 and 19. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 3, 10 and 20.

c. Claim 9

Claim 9 recites, *inter alia*, "generating a first signature by the sender using the hash key and the data" and "compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data." On pages 10-11 of the Office Action, Appellee appears to acknowledge that *Roberts* does not teach or even suggest this limitation. Appellant agrees. However, Appellee asserts that *Bowman* overcomes this deficiency. Appellant respectfully disagrees.

On pages 10-11 of the Office Action, Appellee indicates that the limitation of Claim 9 is disclosed in Col. 7, lines 59-67, of *Bowman*, which is quoted above, and in Col. 9, lines 29-55, which states:

> The secret string, 733 is concatenated in block 736 with the random string, 724. The result is supplied to a key generating secure hash algorithm in block 739, which produces a SHAD 742 (identical to 640 in FIG. 6), which is used as the decryption key. The decryption key is then XORed in block 745 with the encrypted string, yielding the message string 748. The message string is then parsed in block 751, to separate the signature SHAD, 755 (624 in FIG. 6) and the VBC message data, 753. The VBC message data is then parsed by block 759 and output to an order processing block, 763. In order to authenticate the VBC message data, to assure that it has not been tampered with or otherwise corrupted in route from the client to the target URL, for the purpose of security, the following steps are executed. The VBC message data 753 is concatenated with the secret string 733 in block 757 and the concatenated string is supplied to a signature secure hash algorithm 761 which is identical to that indicated in FIG. 6 as 624, to reproduce a signature SHAD 765. The signature SHAD 755 parsed from the message string 748 is then compared

> in block 767 to the signature SHAD 765 reproduced by signature secure hash algorithm 761 to assure that they are identical. Without knowing the secret string it would be impossible for an unlawful third party to duplicate a signature SHAD 755 which matches the signature SHAD 765 created by the recipient=s signature secure hash algorithm 761 using the secret string.

Appellee has not specifically pointed out, and Appellant is unable to determine, where a "first signature" as recited in Claim 9 is included in the cited portion of *Bowman*, much less a "second signature." Moreover, Appellee has not specifically pointed out, and Appellant is unable to determine, where "data" as recited in Claim 9 is included in the cited portion of *Bowman*. As noted above, according to 37 C.F.R. §1.104(c)(2), the pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified. Because the quoted portion of *Bowman* does not appear to teach or even suggest the limitations of Claim 9, which also do not appear to have been properly rejected, the Board should overturn Appellee's rejection of Claim 9.

In addition to the above, on pages 10-11 of the Office Action Appellee appears to acknowledge that neither *Roberts* nor *Bowman*, either alone in combination, discloses "generating a first signature by the sender using the hash key and the data." Indeed, Appellee states that the "difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key" (emphasis in original). However, on page 11 of the Office Action Appellee indicated that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for better security." Appellants disagree. Indeed, if one skilled in the art would have used the hash key instead of the private key to generate better security as suggested by Appellee, then Appellant submits that *Bowman* would have used the hash key instead of the private key to generate the signatures. Because *Bowman* did not use the hash key in favor of the private key, as acknowledged by Appellee, Appellant submits that Appellee's reasoning and rationale for modifying *Roberts* is not well founded. As such, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 9.

Claim 9 depends from and includes all the base limitations of independent Claim 1. As such, Claim 9 is believed to be patentable for at least the reasons noted above for Claim 1. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 9.

d. Claims 16 and 17

Claims 16 and 17 recite, *inter alia*, "receiving a signature from the sender" and Claim 18 recites, *inter alia*, "receiving a first signature from the sender." On pages 13-14 of the Office Action, Appellee indicates that the limitation of Claims 16-18 is disclosed in Col. 7, lines 59-67, of *Bowman*, which states:

> The secret ID, random string, and encrypted VBC string are then concatenated in block 437. In block 438 the concatenated string is character encoded, e.g., by Base 64 encoding, to form the virtual bar code. Base64 encoding has the advantage that the resulting character string is made up of character common to ASCII, EBCDIC and other character sets used by computers around the world through which HTTP messages may be routed.

Appellee has not specifically pointed out, and Appellant is unable to determine, where a "signature" as recited in Claims 16 and 17 or a "first signature" as recited in Claim 18 is included in the cited portion of *Bowman*. According to 37 C.F.R. §1.104(c)(2), the pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified.

Because the quoted portion of *Bowman* does not appear to teach or even suggest the limitations of Claims 16 and 17, which also do not appear to have been properly rejected, the Board should overturn Appellee's rejection of Claims 16 and 17.

Claims 16 and 17 depend from and includes all the base limitations of independent Claim 11. As such, each of Claims 16 and 17 is believed to be patentable for at least the reasons noted above for Claim 11. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 16 and 17.

e. Claims 6, 13, 18, 21, 26 and 28

Claims 6, 13, 18, 21, 26 and 28, either directly or through intervening claims, depends from and includes all the base limitations of independent Claims 1, 11, 19 and 27, respectively. As such, each of Claims 6, 13, 18, 21, 26 and 28 is believed to be patentable for at least the reasons noted above for Claims 1, 11, 19 and 27. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 6, 13, 18, 21, 26 and 28.

CONCLUSION

Appellant has demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Appellant respectfully requests that the Board of Patent Appeals and Interferences reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

The Commissioner is authorized to charge the statutory fee of $540.00 to Deposit Account No. 08-2025 of Hewlett-Packard Company. Although no other fee is believed due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

/James L. Baudino/
James L. Baudino
Reg. No. 43,486

Date: October 10, 2008

Hewlett-Packard Company
Legal Department – MS 4059
19483 Pruneridge Ave.
Cupertino, CA 95014-0604
408-447-0289

CLAIMS APPENDIX

1. A method for secure data transmission, comprising:

generating a character string at a sender for each data packet associated with the secure data transmission;

generating a hash key using the character string and a private key, wherein the hash key is different for each data packet associated with the secure data transmission;

encrypting a data packet associated with the secure data transmission using the hash key; and

transmitting an identification key associated with the sender, the character string, and the encrypted data packet from the sender to a recipient.

2. The method of Claim 1, wherein generating the hash key comprises hashing the character string with the private key.

3. The method of Claim 1, further comprising:

generating a signature using the hash key and the data; and

transmitting the signature from the sender to the recipient.

4. The method of Claim 1, wherein generating a character string comprises randomly generating the character string.

5. The method of Claim 1, further comprising:

determining the private key at the recipient using the identification key; and

decrypting the encrypted data at the recipient using the private key and the character string.

6. The method of Claim 5, wherein determining the private key comprises accessing a relational database associating the identification key to the private key.

7. The method of Claim 1, further comprising:

determining the private key at the recipient using the identification key;

determining the hash key at the recipient using the private key and the character string; and

decrypting the encrypted data using the hash key.

8. The method of Claim 7, wherein determining the hash key comprises hashing the private key with the character string.

9. The method of Claim 1, further comprising:

generating a first signature by the sender using the hash key and the data; and

transmitting the first signature to the recipient, the recipient adapted to determine the hash key for decrypting the data and compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data.

10. The method of Claim 1, further comprising:

generating a signature using the hash key and the data;

transmitting the signature to the recipient;

determining the private key at the recipient using the identification key;

determining the hash key at the recipient using the private key and the character string;

decrypting the encrypted data at the recipient using the hash key; and

verifying the signature at the recipient using the hash key and the decrypted data.

11. A method for secure data transmission, comprising:

receiving a plurality of character strings from a sender;

receiving an identification key from the sender;

receiving a plurality of encrypted data packets from the sender, each of the plurality of character strings correspond to one of the plurality of encrypted data packets;

determining a private key associated with the sender using the identification key; and

decrypting the plurality of encrypted data packets using the private key and the respective character strings.

12. The method of Claim 11, further comprising determining a hash key using the character string and the private key, and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key.

13. The method of Claim 11, wherein determining the private key comprises accessing a relational database associating the identification key to the private key.

14. The method of Claim 11, wherein receiving the character string comprises receiving a randomly generated character string.

15. The method of Claim 11, further comprising hashing the character string with the private key to generate a hash key, and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key.

16. The method of Claim 11, further comprising:

receiving a signature from the sender; and

verifying the signature using the decrypted data, the private key, and the character string.

17. The method of Claim 11, further comprising:

receiving a signature from the sender;

determining a hash key using the private key and the character string; and

verifying the signature using the decrypted data and the hash key.

18. The method of Claim 11, further comprising:

receiving a first signature from the sender;

determining a hash key using the private key and the character string;

generating a second signature using the hash key and the decrypted data; and

comparing the first signature to the second signature.

19. A system for secure data transmission, comprising:

a processor;

a memory coupled to the processor;

a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string;

a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the character string and a private key, wherein the hash key is different for each data packet associated with the secure data transmission; and

an encryption engine stored in the memory and executable by the processor, the encryption engine adapted to encrypt the data using the hash key; and

wherein the processor is adapted to transmit the encrypted data, an identification key related to the private key, and the character string to a recipient.

20. The system of Claim 19, further comprising a signature engine stored in the memory and executable by the processor, the signature engine adapted to generate a signature using the hash key and the data, the processor further adapted to transmit the signature to the recipient.

21. The system of Claim 20, wherein the recipient is adapted to decrypt the encrypted data and verify the signature using the decrypted data.

22. The system of Claim 19, wherein the hashing engine is adapted to hash the character string with the private key to generate the hash key.

23. The system of Claim 19, wherein the string generator is adapted to randomly generate the character string.

24. The system of Claim 19, wherein the recipient is adapted to decrypt the encrypted data using the identification key and the character string.

25. The system of Claim 19, wherein the recipient is adapted to determine the hash key using the identification key and the character string and decrypt the encrypted data using the hash key.

26. The system of Claim 19, wherein the recipient is adapted to access a relational database associating the identification key with the private key and decrypt the encrypted data using the private key and the character string.

27. A system for secure data transmission, comprising:

a processor adapted to receive a plurality of encrypted data packets, an identification key, and a plurality of character strings from a sender, each of the plurality of character strings correspond to one of the plurality of encrypted data packets;

a memory coupled to the processor;

a relational database stored in the memory and accessible by the processor, the relational database relating the identification key to a private key; and

a decryption engine stored in the memory and executable by the processor, the decryption engine adapted to decrypt the encrypted data packets using the respective character strings and the private key.

28. The system of Claim 27, further comprising a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the private key and the character string, the decryption engine adapted to decrypt the encrypted data using the hash key.

29. The system of Claim 27, further comprising a signature engine stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the private key and the character string.

30. The system of Claim 27, further comprising:

a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the private key and the character string; and

a signature engine stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the hash key and the decrypted data.

31. The system of Claim 27, further comprising a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to hash the character string with the private key to generate a hash key, the decryption engine adapted to decrypt the encrypted data using the hash key.

32. The system of Claim 27, further comprising a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string, and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the character string and the private key.

33. The system of Claim 32, further comprising:

a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string; and

a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to hash the character string with the private key to generate a hash key, and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the hash key.

34. The system of Claim 32, further comprising a signature engine stored in the memory and executable by the processor, the signature engine adapted to generate a first signature using the decrypted data and compare the first signature to a second signature received from the sender.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None